

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 843 438 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.05.1998 Bulletin 1998/21

(51) Int Cl.⁶: H04L 9/32, H04N 7/167

(21) Application number: 97402542.1

(22) Date of filing: 27.10.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV RO SI

(72) Inventors:
• Campinos, Arnaldo
92648 Boulogne Cedex (FR)
• Fischer, Jean-Bernard
92648 Boulogne Cedex (FR)

(30) Priority: 13.11.1996 FR 9613822

(71) Applicant: THOMSON multimedia
92648 Boulogne Cédex (FR)

(74) Representative: Ruellan-Lemonnier, Brigitte et al
THOMSON multimedia,
46 quai A. Le Gallo
92648 Boulogne Cédex (FR)

(54) **Process for protecting an information item transmitted from a security element to a decoder and protection system using such a process**

(57) The invention relates to a process for protecting an information item transmitted from a security element to a decoder and a protection system using such a process.

The information item is protected by encrypting

within the security element the information item to be transmitted to the decoder and by decrypting this information item within the decoder.

The invention applies to conditional-access systems.

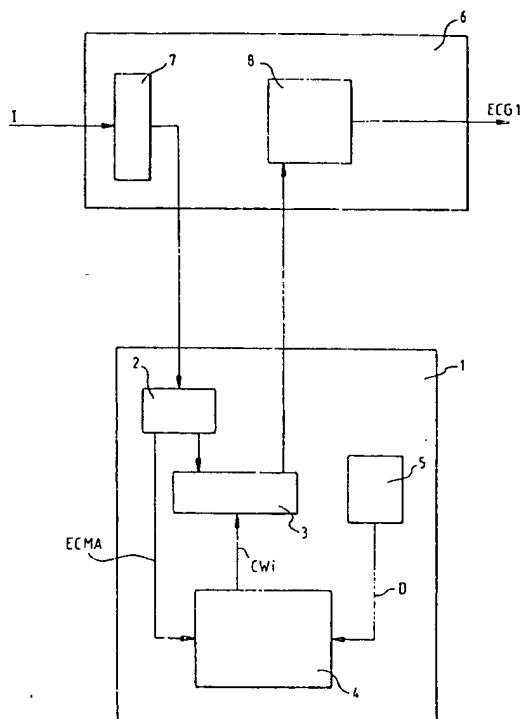


FIG.1

Description

The invention relates to a process for protecting an information item transmitted from a security element such as, for example, a user-card of a conditional-access system, to a decoder.

The invention applies more particularly to conditional-access systems for which the descrambling operation is performed in the security element which is then, for example, a PCMCIA type card complying with the interface standard known by those skilled in the art as "CENELEC/DVB- Common Interface" or a chip card complying with the American NRSS standard (standing for "National Renewable Security System").

The invention applies to any type of conditional-access system, whether this system be of the on-line type or the standalone type.

In an on-line conditional-access system, the scrambled information item is an information item consisting of a signal distributed simultaneously to various users.

In a standalone conditional-access system, the scrambled information item is contained on standalone information media such as, for example, compact discs or digital video discs.

The information item making up the various programmes originating from the issuing source, such as, for example, a service provider, is transmitted to the security element. The security element descrambles the programme selected by the user (provided that the user's entitlements are present in the security element) and sends this programme, as well as the other programmes which have remained unchanged, to the decoder.

Such a process has the drawback that the programme selected by the user is transmitted unencrypted.

Such a transmission can readily be exploited by a pirate who can use it to distribute the pirated programme illegally.

Figure 1 represents the schematic of a security element/decoder assembly according to the prior art.

The system of Figure 1 comprises an information source 1, a decoder 6 and a security element 1.

The decoder comprises a demodulation device 7 and a demultiplexing and decoding device 8.

The security element 1 contains a filtering device 2, a descrambling device 3, an access control device 4 and a user entitlement storage device 5.

The information item 1 issued by the issuing source contains one or more multiplexed programmes, for example, according to the MPEG-2 transport standard (standing for "Moving Picture Expert Group").

As is known to those skilled in the art, the programmes output by the issuing source are scrambled programmes. The information item 1 contains, in messages which will hereafter be denoted ECM, the encrypted control words allowing, after decryption, the descrambling of the scrambled programmes.

After the decoder receives the information item 1, the latter is demodulated by the device 7 and then transmitted in full to the security element 1. The latter filters, with the aid of the device 2, the ECMs (denoted ECMA in Figure 1) corresponding to the programme selected by the user and transmits them to the device 4 for processing. The non-filtered part of the information item is transmitted without modification to the descrambler 3. The device 4 carries out the conventional functions for processing the ECMs, and, in particular, decrypts the control words CWi which they contain, provided that the entitlements D necessary for descrambling the selected programme and output by the device 5 are applied to the device 4.

The control words CWi are subsequently transmitted to the descrambling device 3 which uses them to descramble the programme selected by the user. The information item output by the descrambler 3 is transmitted to the demultiplexing and decoding device 8 so as to generate the usable, i.e., for example, displayable in the case of a film, information item ECG1.

The invention does not have this drawback.

The invention relates to a process making it possible to transfer from a security element to a decoder a stream of data arising from a descrambler included within the security element. The process comprises a first step making it possible to encrypt, in the security element, the information item arising from the descrambler under the action of a first encryption key and a second step making it possible to decrypt, in the decoder, the encrypted information item arising from the first step, under the action of a second encryption key.

The invention also relates to a security element containing a descrambler making it possible to descramble the information item which it receives under the action of control words. The security element comprises a device for encrypting the descrambled information item arising from the descrambler under the action of a first encryption key.

The invention also relates to a decoder making it possible to decode data arising from a security element, the said data representing at least one programme selected by a conditional-access system user. The decoder comprises a decryption device making it possible to decrypt, under the action of a second key, the data arising from the security element, the said data being data which are descrambled and encrypted under the action of a first key.

The invention further relates to an assembly made up of a security element and of a decoder. The security element is a security element according to the invention such as that mentioned above and the decoder is a decoder according to the invention such as that mentioned above.

As has been mentioned earlier, an advantage of the invention consists in protecting the transmission of the programme selected by the user from the security element to the decoder.

Other characteristics and advantages of the invention will emerge on reading embodiments of the invention given with reference to the appended figures in which:

- Figure 1 represents the schematic of a security element/decoder assembly according to the prior art;
- Figure 2 represents the schematic of a security element/decoder assembly according to a first embodiment of the invention;
- Figure 3 represents the schematic of a security element/decoder assembly according to a second embodiment of the invention;
- Figure 4 represents the schematic of a security element/decoder assembly according to a third embodiment of the invention.

In all the figures, the same labels denote the same elements.

Figure 2 represents the schematic of a security element/decoder assembly according to a first embodiment of the invention.

In addition to the elements described in Figure 1, the decoder 6 comprises a decryption device 9 and the security element 1 comprises an encryption device 10. The programme selected by the user is encrypted by the device 10 using an encryption key K. Conversely, the device 9 decrypts the programme with the help of the same key K. Advantageously, this avoids having transmission of the programme unenciphered between the security element and the decoder.

According to the invention, the encryption and decryption key K can be common to all the security element/decoder pairs, but can also be specific to each pair or group of security element/decoder pairs. Advantageously, the production of pirate clones of security elements is thereby impaired.

Thus, this technique forces pirates to customize each of their clones on the basis of the decoder to which they are connected. This has the consequence of complicating their task and hence of reducing the rewards which they may derive from piracy.

According to a particular implementation of the embodiment of Figure 2, a public key algorithm can be used for the devices 9 and 10. In this case, the encryption key is different from the decryption key and, in a preferred manner, the secret key is used for encryption in the security element while the public key is used for decryption in the decoder.

According to this first embodiment of the invention, the key K is a key stored permanently both in the security element and in the decoder.

Figure 3 represents the schematic of a security element/decoder assembly according to a second embodiment of the invention.

In addition to the elements described in Figure 2, the decoder comprises a device 11 for generating a random number or random words AL and a device 12 for

generating decryption keys and the security element comprises a device for generating encryption keys 13.

Instead of using a fixed key K, as in Figure 2, the encryption and decryption keys are here generated dynamically. To do this, the decoder 6 generates a random number AL by way of the device 11 and transmits it to the device 13 of the security element. Moreover, the device 11 transmits the random number to the device 12. The latter encrypts the random number AL under the action of a key K1 so as to give the decryption key K. In the same way, the device 13 of the security element encrypts the random number under the action of a key K1 and produces the encryption key K.

According to a particular embodiment of the invention, described in Figure 3, the encryption algorithm used by the devices 12 and 13 can be replaced by a "one-way" function with key K1. Such a function is for example described in the European patent application filed under number 96401336.1-2209.

Advantageously, the devices 12 and 13 prevent any pirate from discovering the encryption/decryption key K solely through the data item AL which travels between the decoder and the security element.

According to another particular embodiment of the invention, the key K1 used by the devices 13 and 12 can be specific to the security element/decoder pair, thus exhibiting the advantages mentioned earlier.

According to another particular advantageous embodiment of the invention, the procedure for generating the encryption and decryption key K can be renewed each session or else several times per session. Session should be understood to be an uninterrupted sequence of reception of one and the same programme by a user.

These renewals of the keys K exhibit, among other things, the following benefits:

- on the one hand, they make it possible to increase the soundness of the encryption/decryption algorithm of the devices 9 and 10. Soundness of the algorithm should be understood to be the resistance of the algorithm to piracy by cryptanalysis.

The frequency of renewal of the keys directly influences the amount of data encrypted with the same key made available to a pirate so as to cryptanalyse the algorithm. Since limiting this amount increases the resistance of the algorithm to attacks, frequent renewals of the key K increase the soundness of the encryption/decryption algorithm of the devices 9 and 10.

- on the other hand, it makes it possible to avoid replaying previously selected programmes.

Thus, if an ill-intentioned user or a pirate records the information output by the device 10, and therefore records, at the instant t, the selected programme in a form encrypted with a key denoted K_t, he will not be able to use the said programme subsequently since the de-

ryption key at the instant $t+\Delta t$, denoted $K_{t+\Delta t}$, will be different from the encryption key K_t .

Figure 4 represents the schematic of a security element/decoder assembly according to a third embodiment of the invention.

In addition to the elements described in Figure 2, Figure 4 includes, in respect of the decoder, a random number generator 11 and an encryption device 14 and, in respect of the security element, a decryption device 15.

The generator 11 generates a random number AL which is used directly as decryption key K by the device 9. Moreover, the random number AL is transmitted to the device 14 which encrypts it and transmits it to the device 15 of the security element. The encryption performed by the device 14 is performed under the action of a key K2. On the security element side, the encrypted random number E(AL) is decrypted by the device 15 under the action of a key K2 and the result AL is transmitted to the device 10 so that it serves as encryption key K.

According to another embodiment of the invention, a public key algorithm can be used for the devices 14 and 15. In this case, the encryption key is different from the decryption key and, in a preferred manner, the secret key is used for decryption in the device 15 whilst the public key is used for encryption in the device 14.

Advantageously, the devices 14 and 15, whether they use a symmetric algorithm or a public key algorithm, prevent any pirate from discovering the encryption/decryption key K merely by knowing E(AL).

According to the particular embodiments of the invention which were mentioned earlier:

- the random number AL can be generated once per session or indeed several times during the same session;
- the encryption/decryption key K2 used by the devices 14 and 15 can be made specific to the security element/decoder pair, thus exhibiting the above-mentioned advantages.

In the context of the invention, for all the embodiments described in Figures 2, 3 and 4, the choice of the encryption/decryption algorithm of the devices 9 and 10 results from a compromise between the desired level of protection of the programmes and the complexity of the algorithm implemented in the decoder and in the security element.

Thus, a symmetric algorithm which is simple to implement via a dedicated circuit is preferred. Such an arrangement makes it possible, advantageously, to reduce the cost of implementation and to ensure high encryption/decryption rates, for example of the order of about ten Megabits per second. Renewal of the encryption keys then advantageously allows the use of a simple algorithm while decreasing the risks of piracy by cryptanalysis.

Furthermore the systematic decryption performed

by the device 9 of the decoder exhibits a particular benefit, viz. that the user can display, via the decoder, only the programmes originating from the security element. This implies, for example, that unenciphered pirate programmes may not be played on the decoder alone.

In the case in which the keys K1, K2 are specific to each security element/decoder pair, the abovementioned property of systematic decryption has an additional advantage, viz. of preventing any pirate from supplying the same programme to decoders which are different from the decoder which he has pirated.

Moreover, for all the embodiments of the invention described in Figures 2, 3 and 4, the implementation consisting in integrating the devices 8 and 9 into the same electronic circuit will be preferred. This is so as to preclude the contents of the selected programme from appearing unenciphered between the two devices.

Claims

1. Process making it possible to transfer from a security element (1) to a decoder (6) a stream of data arising from a descrambler (3) contained in the security element (1), the said stream of data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a first step making it possible to encrypt in the security element (1) the data arising from the descrambler (3) under the action of a first key (K) and a second step making it possible to decrypt in the decoder (6) the encrypted information item arising from the first step, under the action of a second key (K).
2. Process according to Claim 1, characterized in that the first step comprises a step making it possible to generate random words (AL) in the decoder and a step making it possible to encrypt the random words generated (AL) under the action of a third key (K1) in such a way as to generate the first key and in that the second step comprises a step making it possible to encrypt the random words (AL) in such a way as to generate the second key (K).
3. Process according to Claim 1, characterized in that the first step comprises a step making it possible to generate at least one random word (AL) in such a way that this random word constitutes the first key (K) during the whole of the descrambler (3) descrambling session and in that the second step comprises a step of encryption of the random word (AL) under the action of a fourth key (K2) in such a way as to make up an information item made up of an encrypted random word (E(AL)), and a step consisting of the decrypting of the encrypted random word (E(AL)) in such a way that the decrypted random word constitutes the second key (K).

4. Process according to Claim 1, characterized in that the first key (K) is stored permanently in the user-card (1) and in that the second key (K) is stored permanently in the decoder (6). 5
5. Security element (1) containing a descrambler (3) making it possible to descramble the data which it receives under the action of control words (Cw_i), the said data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a device (10) for encrypting the descrambled information item arising from the descrambler (3) under the action of a first encryption key (K). 10 15
6. Security element (1) according to Claim 5, characterized in that it comprises a device for generating encryption keys (13) making it possible to generate the first key (K) under the action of a random word (AL). 20
7. Security element (1) according to Claim 5, characterized in that it comprises a decryption device (15) making it possible to generate, under the action of a decryption key (K2), the first key (K). 25
8. Decoder (6) making it possible to decode data arising from a security element (1), the said data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a decryption device (9) making it possible to decrypt, under the action of a second key (K), the data arising from the security element (1), the said data being data which are descrambled and encrypted under the action of a first key (K). 30 35
9. Decoder (6) according to Claim 8, characterized in that it comprises a generator (11) of random words generating at least one random word (AL) and a device for generating decryption keys (12) from the random word thus generated, in such a way that the decryption key arising from the said generating device (12) is the second key (K). 40
10. Decoder (6) according to Claim 8, characterized in that it comprises a generator (11) of random words making it possible to generate at least one random word making up the second key (K) and an encryption device (14) making it possible to encrypt the random word making up the second key under the action of an encryption key (K2). 45 50
11. Assembly made up of a security element (1) and of a decoder (6) associated with this security element, characterized in that the security element is a security element (1) according to Claim 6 and in that the decoder (6) is a decoder according to Claim 9. 55
12. Assembly made up of a security element (1) and of a decoder (6) associated with this security element, characterized in that the security element is a security element (1) according to Claim 7 and in that the decoder (6) is a decoder according to Claim 10.
13. Assembly according to Claim 11 or 12, characterized in that the first key and the second key are keys specific to the said assembly.

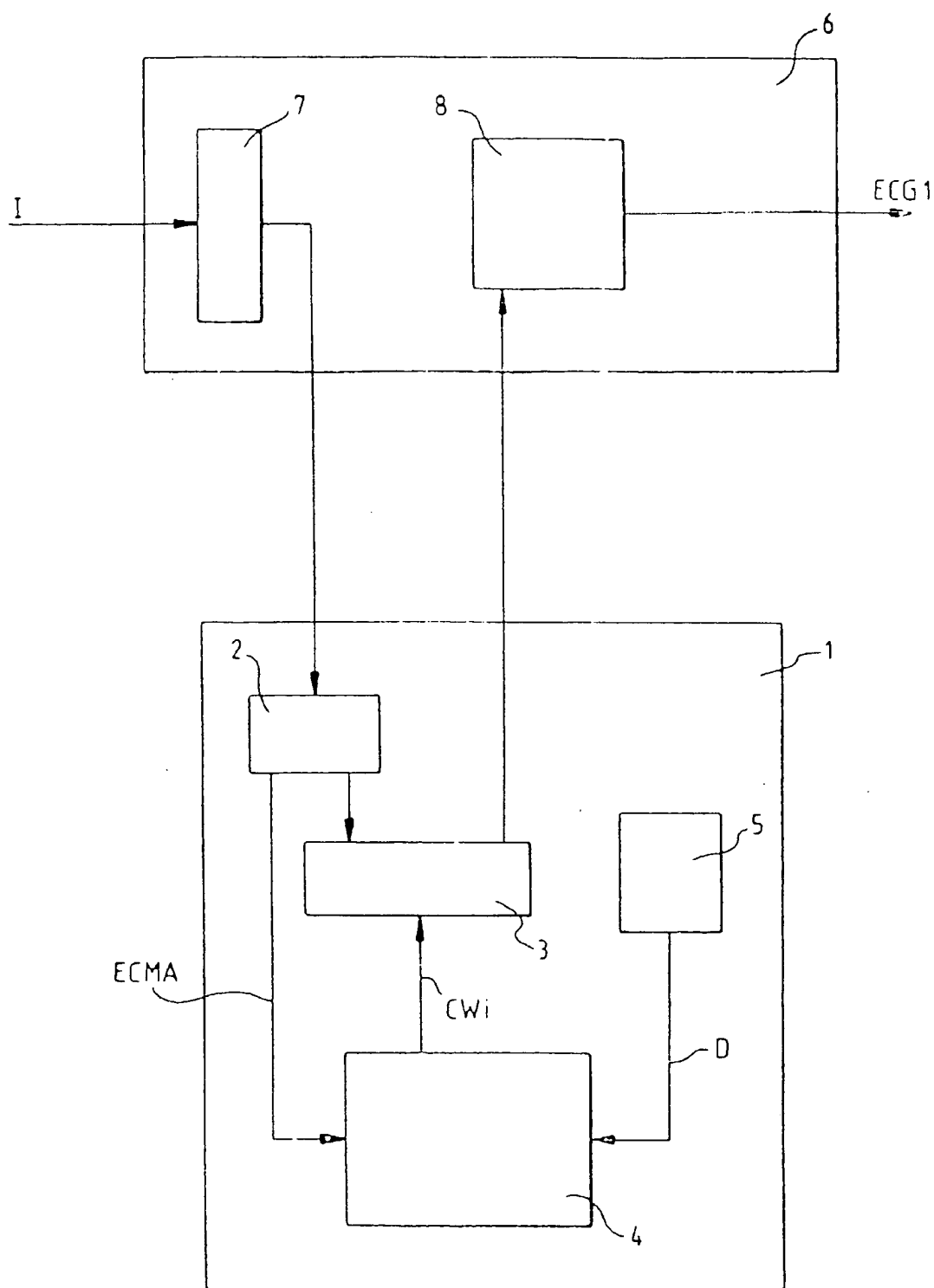


FIG.1

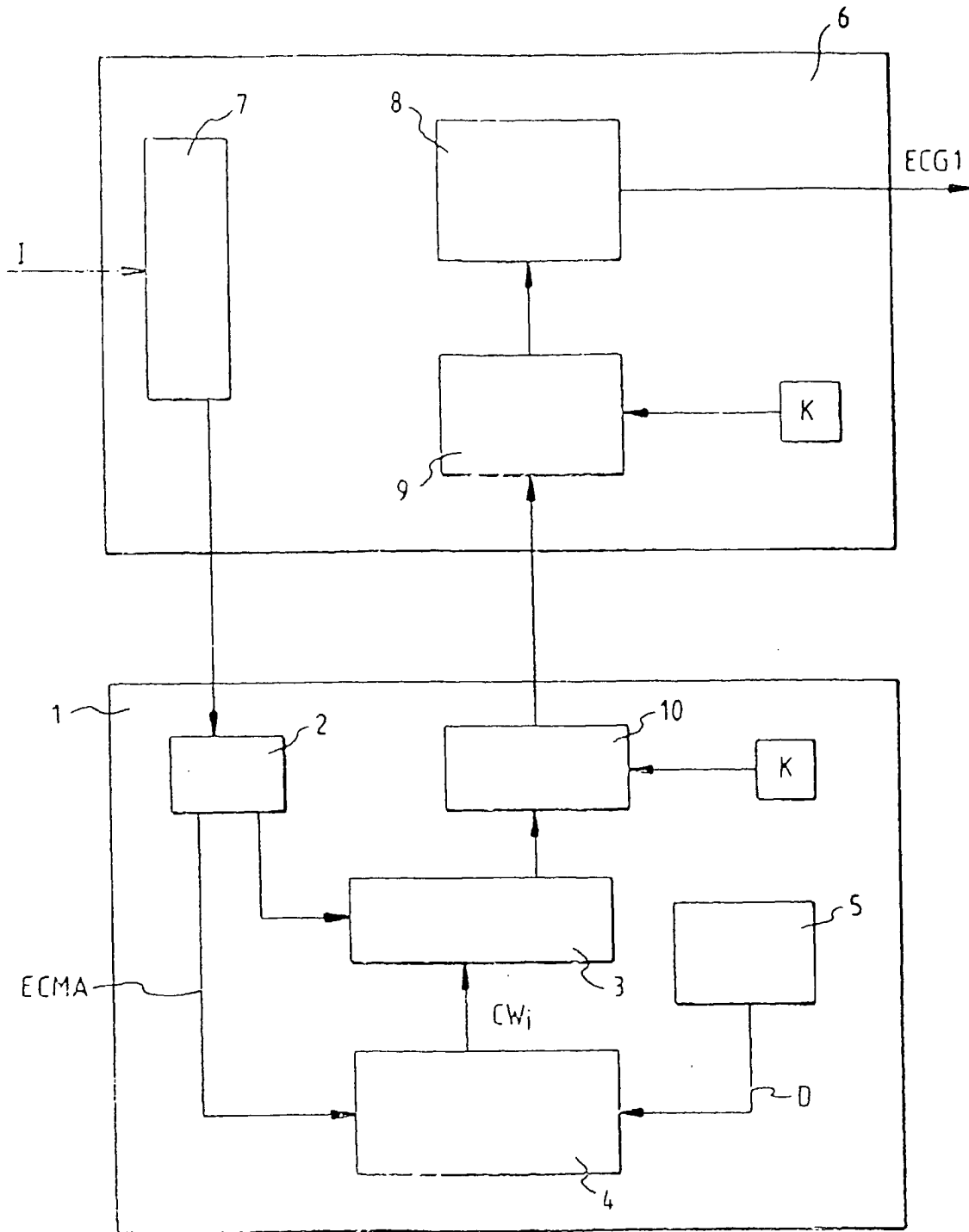


FIG.2

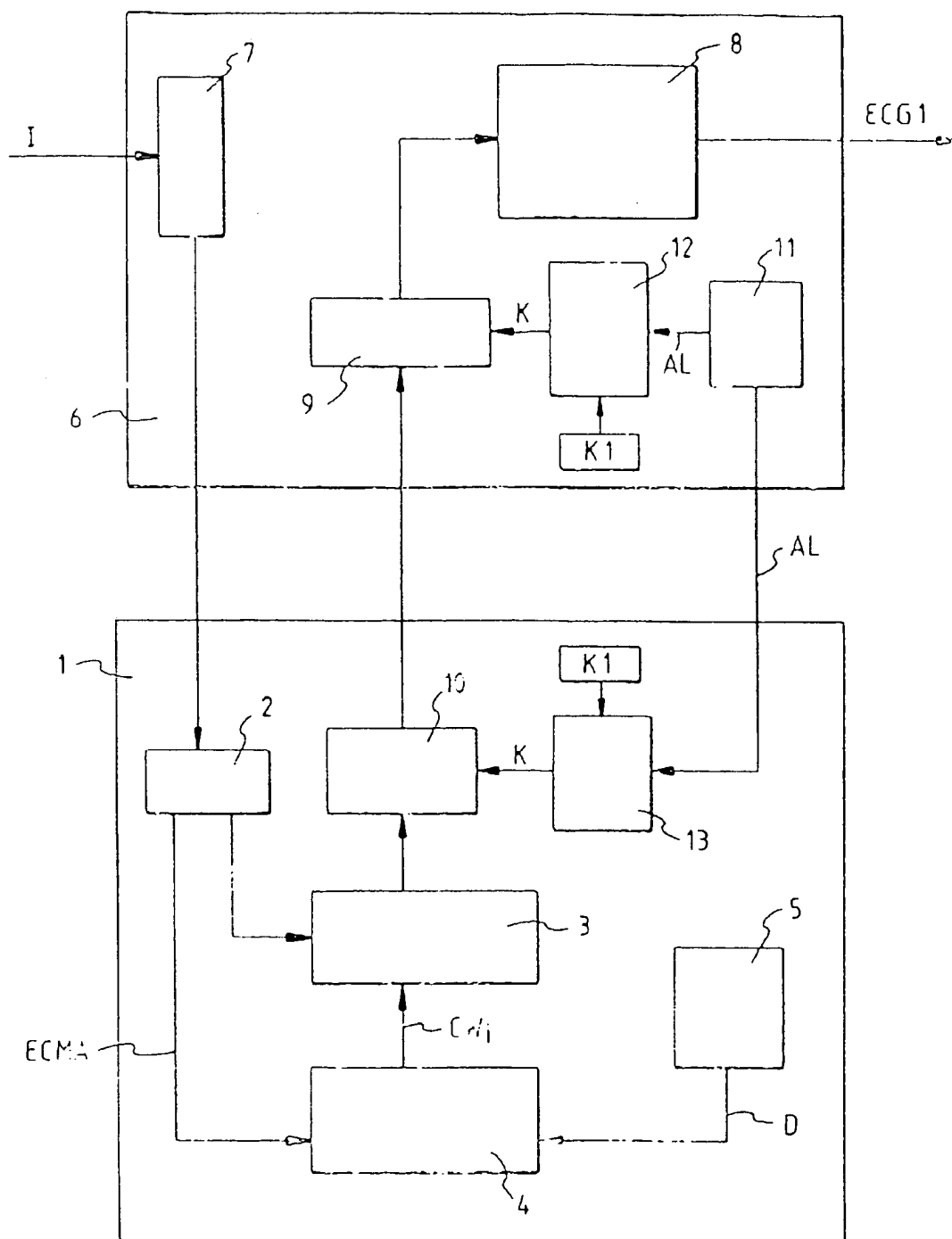


FIG.3

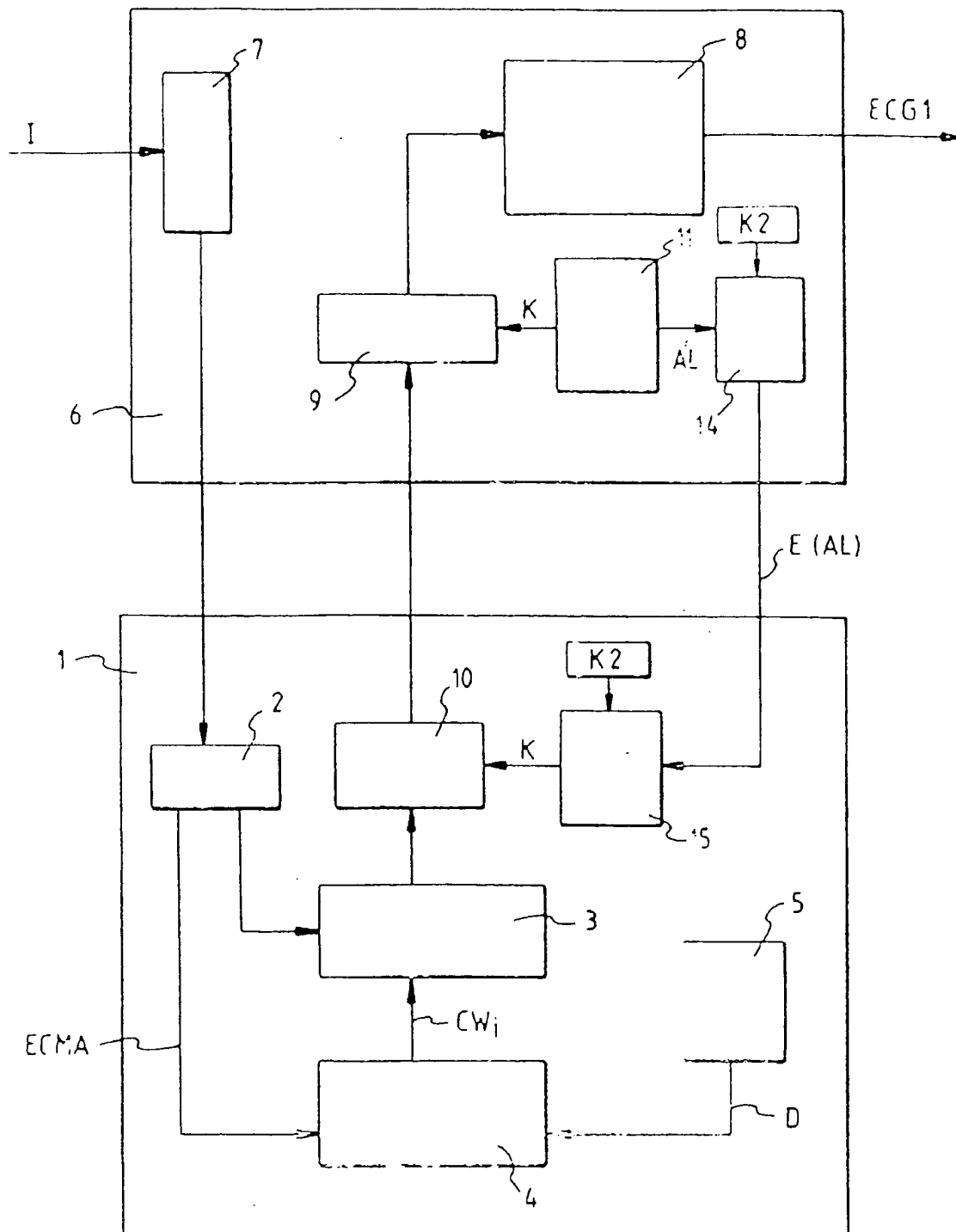


FIG. 4